Department of
INFORMATION
TECHNOLOGY

Maryland Media Protection Policy

Last Updated: 06/09/2017

Contents

1.0 Purpose

The Maryland Department of Information Technology (DoIT) is responsible for, and committed to, managing the confidentiality, integrity, and availability of State government information technology (IT) networks, systems, and applications within the scope of its authority. As part of the commitment to confidentiality, DoIT is focused on protecting Executive Branch agencies against information loss by ensuring data is tracked and access is limited to only those personnel with **need-to-know**.

This policy directs DoIT and Executive Branch agencies to control portable and writeable media assets, such as external hard drives, DVDs, and USB flash drives, to minimize the risk of confidential data loss and to reduce the risk of unauthorized disclosure resulting in a possible data breach. To protect information assets, DoIT will utilize the baseline controls and standards established by NIST Special Publication (SP) 800-53R4, SP 800-88R1, and SP 800-111 to categorize assets.

2.0 Document and Review History

This policy supersedes the Maryland Information Security Policy v3.1 (2013), Section 6.5: Media Protection and any related documentation regarding media protection declared prior to the 2017 Cybersecurity Program Policy. This document will be reviewed annually and is subject to revision.

Date	Version	Policy Updates	Updated By:
01/31/2017	v1.0	Approval of Draft	Maryland CISO
06/09/2017	v1.1	Initial Publication	Maryland CISO

3.0 Applicability and Audience

It is the responsibility of every user to protect confidential information from unauthorized disclosure; and agencies, as data owners, must ensure both portable (e.g., removable) and writable media containing confidential information is controlled, tracked, securely stored, and properly disposed of. This policy is applicable to all IT environments and assets owned or operated by any agency supported by, or under the policy authority of, the Maryland Department of Information Technology. Agencies under the policy authority, but not under direct management of DoIT, must independently comply with the requirements of this policy.

4.0 Policy

Writable media, such as DVDs, USB flash memory, and external hard drives, have become common tools in IT environments, but the portability that makes them useful and convenient presents a serious risk of data loss or breach. Users with write-access to media can transfer confidential data to a disc or memory card and walk out the door with it, either maliciously stealing the information or accidentally exposing the media to possible compromise. The lack of strong data-management poses significant risks to controlling agency information and incurs potential financial liability should the information be disclosed.

The *DoIT Asset Management Policy* directs agencies to establish a software media library or repository, which must be controlled by an agency asset-manager or designated custodian, for **information media assets**. The *DoIT Data Security Policy* ensures procedures and baselines are established to track information flow across the network and to detect unauthorized locations for data-at-rest. This media protection policy establishes the requirements that ensure users are accountable for protecting confidential information on portable and writable media and that agencies implement security controls for managing how this media, and its data, are stored, transferred, accessed, and properly destroyed when no longer needed.

As identified in the *DoIT Asset Management Policy*, information technology assets for Enterprise onboarded agencies are managed by the Enterprise Asset Manager. The Enterprise Asset Manager may designate a local, onsite software media-library custodian for each agency. The custodian may have visibility into the type of information the agency processes and can assist in ensuring media is protected at the level required by its classification. Non-Enterprise agencies under the policy authority but not under direct management of DoIT must independently comply with the requirements of this policy.

4.1 Data Security

Network controls will be implemented to limit access to portable media devices. Due to the inherent interconnectedness of systems in a trusted network, users may have access to data stores, shared applications, and network-available resources, and a subset of those users would probably require the ability to burn CDs or DVDs or store data on USB flash memory drives or external hard drives. However, portable media shall not be used to transfer confidential or sensitive data among parties if an electronic means of secure file transfer is, or can be made, reasonably available.

System administrators will use group policies, security templates, and other controls to disable portable media capabilities and ensure monitoring capabilities are present to detect changes in account permissions. By restricting access to administrative interfaces and devices, the likelihood of users accidentally or maliciously infecting systems through these vectors is reduced.

Technical and administrative requirements listed below will be implemented to help reduce the risks associated with using portable and writeable media.

#	Name	Requirement
A	Disable USB access	Users will be restricted from using USB ports on workstations, except for default keyboard/mouse devices.
B	Disable CD/DVD drive access	Users will be restricted from using optical drives on workstations, this includes magnetic drives like floppy or zip disk drives.
C	Disable Media Ports	Users will be restricted from using media ports such as SD memory, Micro-SD, and flash memory interfaces on workstations.

#	Name	Requirement
D	Disable Unneeded Connectors	Users will be restricted from using connectors like parallel or serial ports on workstations, though video interfaces may be allowed, such as HDMI or VGA ports.
E	Establish Controlled-Membership Groups	▪ Administrators will establish security groups to control access to required interfaces; security training will be required for group membership. ▪ Control-group members (i.e., the authorized users) will be identified as Designated Media Agents and will provide the extended security functions described in key sections within this policy
F	Membership Auditing	▪ Security groups will be audited periodically by the Enterprise ISSM to ensure only approved users have membership; manager approval will be required ▪ The Enterprise ISSM will maintain records of user attendance at yearly security training for those who require access to writeable or portable media
	Required Security Training	Designated Media Agents will be instructed on the following topics and be required to attend yearly training to ensure compliance: ▪ Tracking portable media — from issuance to disposal — in accordance with the media-library logging procedures ▪ Conducting malware scans before accessing media ▪ Encryption procedures, if required ▪ Data classification requirements

4.2 Data Loss Protection

Agencies will ensure that data loss prevention solutions track data being exported to portable assets (e.g., mobile devices or writeable media) and identify user, system, time and date, and file and folder names. Asset managers or designated custodians will issue control numbers to portable media which will be tracked in a software library media-control log. Section 4.4 contains the detailed requirements for this (asset) tracking.

Correlating data exfiltration (transfer to portable media) to the media-control log ensures all transfers are authorized and documented. Any unauthorized data exfiltration will be considered a security violation and investigated. Within the DoIT Enterprise, the Security Operations Center will ensure alerts are generated for any attempt to access data via a (portable) media interface, such as USB or DVD drive, as this may indicate an attempt to compromise the system.

4.3 Importing Data

Users may need to introduce media from external sources into the system, such as files on a DVD or USB memory stick from attending a conference, or media provided by a vendor after purchasing a product. In these cases, users will be required to submit the media to the Enterprise ISSM or a Designated Media Agent for scanning and uploading to a network share; depending on the type of files, individual exceptions may be granted by the Enterprise ISSM.

Media submitted for scanning will be allowed at least a 24-hour turnaround time to ensure data is safe and that contents are classified appropriately, but the scanning should be as expeditious as possible to avoid impeding normal business workflow.

4.4 Controlling Portable and Writeable Media Assets

In addition to the requirements identified in the DoIT Asset Management Policy regarding State-owned software and licenses, portable and writable media will be managed and tracked from issuance through disposal, including destruction. All portable media such as external hard drives, diskettes, CDs/DVDs, and tapes, when procured, will be presented to the agency asset manager for media management and may be added to the software library and subject to maintenance, such as updates to deployed software. The asset manager will ensure inventory tracking and logging is controlled for portable and writeable media as indicated in the table below.

#	Name	Requirement
A	Media Control Log	Maintain an access-controlled log of users who request portable media that can be audited by the ISSM and contains the information identified below as well as any other descriptor that may be required by process improvement or agency-specific functions.
B	Control Number	Issue a unique control number that can be tracked and traced through the log; this may be a label attached to the media, i.e., diskette or backup tape, or a written number in permanent marker such as on a DVD.
C	Date and Time	▪ Record the date and time the media is issued ▪ Record the date and time the media is returned for destruction or storage ▪ Indicate if media is released to a third party and not expected to return
D	Name	Identify the user’s name and agency or department.
E	Purpose	Document the stated purpose of the portable media, e.g., downloading virus updates or using a USB flash memory drive to create a secondary, offline copy of a project.
F	Report of Loss or Theft	▪ Users will report lost or stolen media assets to the Asset Manager as soon as possible ▪ The Asset Manager will document the loss and report it to the ISSM and Data Owners

4.4.1 Writeable Media

The asset manager will track issued media and, when no longer needed, will collect and properly dispose of them, such as shredding DVDs, to ensure no confidential information can be retrieved. This will ensure data that is transferred to a portable medium is tracked and destroyed instead of casually tossed in a trash bin. Dumpster diving (the process of looking through garbage for confidential or valuable information by an adversary) may reveal confidential information that can be used to compromise the network, e.g., specifics of information technology assets used, the type of information handled (PII or PHI), and the specific controls or software used in an environment.

Writeable media will be audited each quarter to ensure data is controlled, and users with media assets assigned will be required to present the media for inventory verification, submission to the software library, or destruction.

4.4.2 Portable Media

Storage media includes USB flash memory drives, external hard drives, and memory cards such as those used in cameras and video recorders, cellphones, and some printers. These devices typically offer much larger storage capabilities — from 500 megabytes to 5 terabytes in size. Storage media can be used for quick, large file transfers or for long-term or backup storage of directories and software.

Controlling access to these devices will provide protection against large-scale data theft, information destruction, or unauthorized modification by an internal user.

Ensuring only authorized users can access the USB functions on systems reduces the risk of users connecting personal storage media and introducing malicious software to the Maryland network, either accidentally or maliciously.

- Asset managers will ensure portable media are controlled by keeping unissued media in a locked container, such as a safe or locked cabinet
- Media will be classified based on the type of confidential information stored on it and only authorized users will have access to the media

This restricts users from accessing confidential information stored on media that they may not have access to on the network. For instance, a user from the Department of Budget and Management may have approval to access financial information (privileged business information) but not to access to payroll data (PII), so that user would not be allowed to use media with PII information.

4.5 Data Sanitization

Asset managers will coordinate with the ISSM to ensure any portable media being repurposed (reused by another agency or department) is properly sanitized to prevent transfer of confidential data to unauthorized parties. Otherwise, all portable and writeable media with confidential information will be properly destroyed to prevent unauthorized exposure of confidential data. All electronic storage media must be sanitized in accordance with NIST SP 800-88R1 “Guidelines for Media Sanitization” and in compliance with the agency’s document-retention policy and litigation hold procedures.

NOTE: Disposal decisions should be made based upon the classification of the data, level of risk, and cost to the agency. Additionally, the procedures performed to sanitize electronic media should be documented and retained to enable audit verification. For more information on data sanitization, see the *DoIT Auditing and Compliance Policy*.

5.0 Exemptions

This policy is established for use within the DoIT Enterprise. If an exemption from this policy is required, an agency needs to submit a DoIT Policy Exemption Form and clearly articulate the reason for the exemption. An operational risk assessment will be conducted to identify the risks and the agency’s mitigation strategy associated with this exemption. If the agency can accept the risk, an exemption to this policy may be granted.

6.0 Policy Mandate and References

The Cybersecurity Program Policy mandates this policy. Related policies include:

- Asset Management Policy
- Auditing and Compliance Policy
- Data Security Policy

7.0 Definitions

Term	Definition
Information Media Assets	Digital media types that include, for example, diskettes, magnetic tapes, external/removable hard disk drives, flash memory drives, compact disks (CDs), and digital video disks (DVDs).
Need-to-Know	Security principle that confidential Information will only be given to people who need it to do a specific job.

8.0 Enforcement

The Maryland Department of Information Technology is responsible for managing information security for the DoIT Enterprise per established requirements authorized in the DoIT Cybersecurity Program Policy. Agencies not directly managed by DoIT must implement due diligence and due care to comply with the minimum requirements identified within this policy. Any agencies under the policy authority of DoIT with requirements that deviate from the DoIT Cybersecurity Program policies are required to submit a Policy Exemption Form to DoIT for consideration and potential approval.

If DoIT determines that an agency is not compliant with this policy, the agency will be given a sixty (60) day notice to become compliant or at least provide the DoIT a detailed plan to comply within a reasonable time before the issue is reported to the Secretary of Information Technology. After which, the Secretary of Information Technology, or a designated authority, may extend a non-compliant agency's window of resolution or revoke an agency or third-party's authority to operate on DoIT resources until such time the agency becomes compliant.

Any personnel attempting to circumvent this policy, such as stealing property — including media designated for disposal, failing to record acquisition, removing media assets from inventory records, or attempting to connect unauthorized media assets to any State-owned system, will be investigated and subject to possible disciplinary action, which may include written notice, suspension, termination, and possible criminal and/or civil penalties.